## REMARKS

In response to the Office Action dated August 27, 2004, Applicant respectfully requests reconsideration and withdrawal of the rejections of the claims.

The Office Action requested the Applicant to furnish a drawing under 37 C.F.R. §1.81. In response thereto, a drawing comprising Figures 1 and 2, corresponding to the two disclosed embodiments, is being submitted herewith. It is respectfully submitted that this drawing does not introduce any new subject matter.

Claims 1-3 and 5-8 were rejected under 35 U.S.C. §102, on the grounds that they were considered to be anticipated by published International Application WO 97/04412, identified as "Williams". Claims 4 and 5 were rejected under 35 U.S.C. §103, as being unpatentable over the Williams reference in view of the LeRoux patent (U.S. 6,182,205). Claim 9 was identified as containing allowable subject matter, which is noted with appreciation.

For the reasons presented below, it is respectfully submitted that the Williams reference neither anticipates, nor otherwise suggests, the claimed subject matter, whether considered by itself or in combination with the LeRoux patent.

As noted in the Office Action, the Williams reference discloses an approach for protecting software against copying, by splitting the software into two parts and separately executing the two parts with different processors. It is respectfully submitted, however, that the particular manner in which the Williams reference carries out this procedure is different from the claimed subject matter.

For example, claim 1 recites that the second, secret part of the program is placed on a secure medium of a second processing means, and that this second

processing means is a portable and detachable accessory chip medium[1]. For example, as disclosed at page 5, lines 22-24 of the original specification, the secret part of the program is disposed in the EEPROM memory of the chip card. To execute the program, the chip card is connected to a PC by means of a suitable interface, such as a card reader, to permit bidirectional communication between them.

The Williams reference does not disclose that a portion of the program is stored on a detachable chip card. Rather, it discloses that, each time the program is to be executed, the secure part of the program is downloaded via a network into the memory 206 of a hardware key 122. The Williams reference does not suggest that the hardware key 122 comprises a chip medium that can be connected to and detached from the processor 102.

In this regard, the Office Action notes that the Williams reference discloses that the hardware key can have chip cards attached, with reference to page 6, lines 31-33. However, the reference does not disclose that these chip cards contain the second, secure part of the program. Rather, the reference only discloses that the secure part of the program resides within the memory 206 of the hardware key 122. As can be seen in Figure 2, this memory is separate from the interface 208 to which the chip cards 124 are connected. Insofar as the chip cards are concerned, the reference discloses that they can be used to supply the unique address associated with the hardware key. See page 7, lines 19-23. There is no suggestion that the chip cards themselves also contain the secure part of the program.

[1] This latter recitation originally appeared as a "wherein" clause at the end of the claim. The claim has been amended to incorporate the recitation into the body of the claim. This amendment does not alter the substantive scope of the claim.

For at least this reason, therefore, it is respectfully submitted that the Williams reference does not anticipate the subject matter of claim 1. For the same reasons, it is also submitted that claim 2 is not anticipated.

In addition to the foregoing distinction, claims 1 and 2 recite other differences between the subject invention and the disclosure of the Williams reference. For example, the approach disclosed in the Williams reference is based upon non-persistent existence of the secure part of the program within the memory of the computer system. As noted at page 4, lines 30-31, the second part of the software must be reloaded *each* time the computer system is powered up. Once the user terminates the use of the application software, the second part of the program is erased from the memory 206 of the hardware key (page 9, line 33 to page 10, line 3). Alternatively, the second part of the program disappears when power is removed from the hardware key, indicating that it is only stored in volatile memory. Thus, the Williams patent clearly teaches against any type of permanent storage of the second part of the program. In order to execute the program, the approach employed in the Williams patent requires the user to be connected to a network.

In contrast, in one embodiment of the present invention, the secret part of the program is stored in the non-volatile memory of the chip card, in which it is executed. As a result, it is not necessary for the user to be connected to a network, in order to utilize the program. Rather, the user only needs to place the chip card in communication with the first processing means, e.g. a personal computer, for example by means of a card reader. It is respectfully submitted that the Williams reference teaches away from the non-volatile storage of the secure part of the program with the second processing means, as recited in claim 1.

In accordance with another embodiment of the present invention, the secure part of the program is encoded, and stored with the public part of the program on the same medium. When the program is to be executed, the encoded secure portion of the program is transmitted from the first processing means to the second processing means, where it is decoded, for example in accordance with an encryption key stored on the second processing means. The decoded version of the secured part of the program is then executed on the second processing means.

It is respectfully submitted that the Williams patent does not disclose this claimed subject matter. The Office Action refers to the fact that the Williams reference discloses that the secure part of the program can be encrypted while it is transmitted to the hardware key. However, the reference does not disclose that the encrypted version of the program is stored together with the public part of the program, on the same medium. Rather, the two portions of the program are separately transmitted to the respective portions of the computer system 100 within which they are executed.

Furthermore, the Williams reference does not disclose that the encoded portion of the program is transmitted from the first processing means to the second processing means, as recited in claim 2. Rather, the hardware key 122 (the second processing means) independently receives the encrypted portion of the program from the network. There is no suggestion that the first processing means 102 ever receives the encrypted portion and transmits it to the hardware key.

For these additional reasons, therefore, it is respectfully submitted that claims 1 and 2 are not anticipated by the disclosure of the Williams reference.

Further distinctions between the subject invention and the Williams reference are set forth in the dependent claims. In view of the fundamental differences presented above, a detailed discussion of these other distinctions is believed to be unnecessary at this time.

Reconsideration and withdrawal of the rejections, and allowance of all pending claims are respectfully requested.

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

Date: November 29, 2004

By: _____
James A. LaBarre
Registration No. 28,632

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620

**AMENDMENTS TO THE DRAWINGS:**

Please add accompanying new Figures 1 and 2 to the application, pursuant to the Examiner's request.